

Columbia Accident Investigation Board (CAIB) Safety System Findings:

Theoretical Bases and Implications for Project Management at NASA

NASA Project Management Challenge 2005
March 22-23, 2005

- Background
- Introduction
- Normal Accident Theory (NAT)
- High Reliability Organization (HRO)
- Naval Reactors (NR)
- Overall NAT and HRO Takeaways
for Project Management
- Additional Reading



- Two challenging CAIB recommendations, from the standpoint of project management, are those involving safety management
 - 7.5-1, Office of Safety Management Enhancement
 - 7.5-2, Independent Technical Authority
- The detailed findings provide enough information for an “organizational checklist”—however, the CAIB went further

Background (contd.)

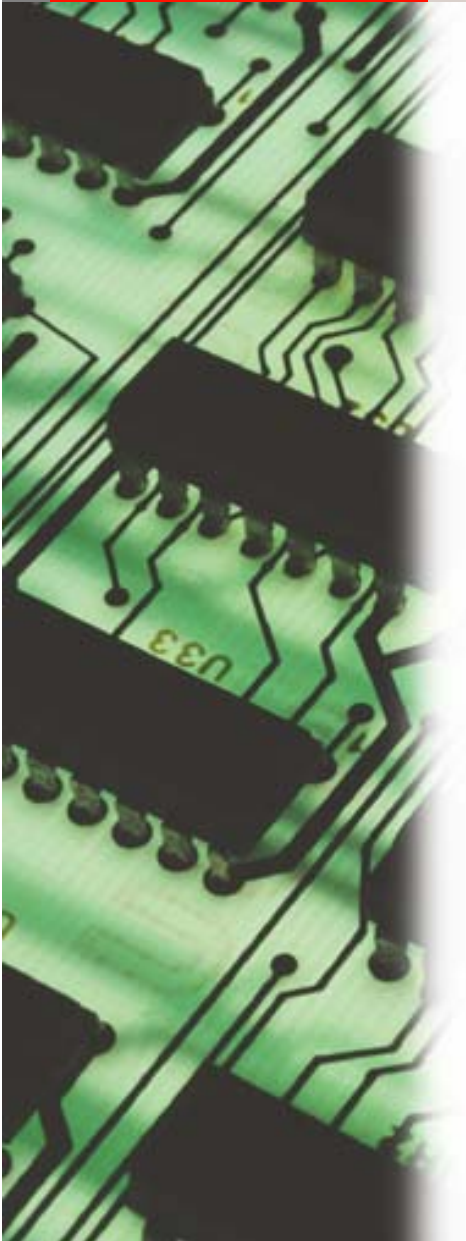


- CAIB:
 - Outlined the theoretical underpinning for its recommendations
 - Highlighted two government organizations that had coupled exemplary safety records with mission success
- CAIB suggested that the essential safety concepts, embodied in the theories they discussed and implemented in the two highlighted government programs, should be embraced by NASA

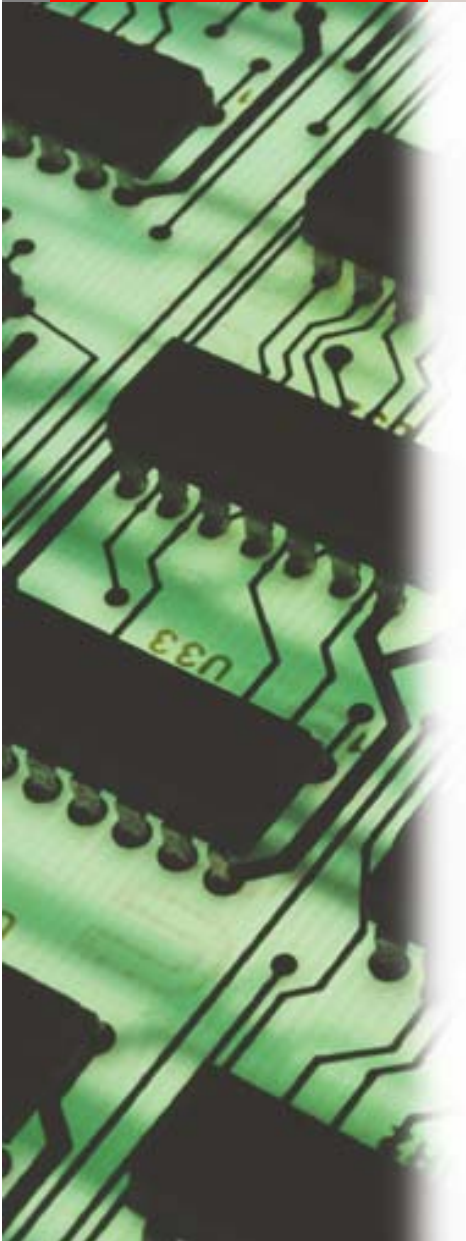


- Review the two safety management theories called out by the CAIB (along with their implications):
 - Normal Accident Theory
 - High Reliability Organizations
- Describe one of the two organizations highlighted as examples by CAIB: Naval Reactors
- Provide thoughts for NASA project management

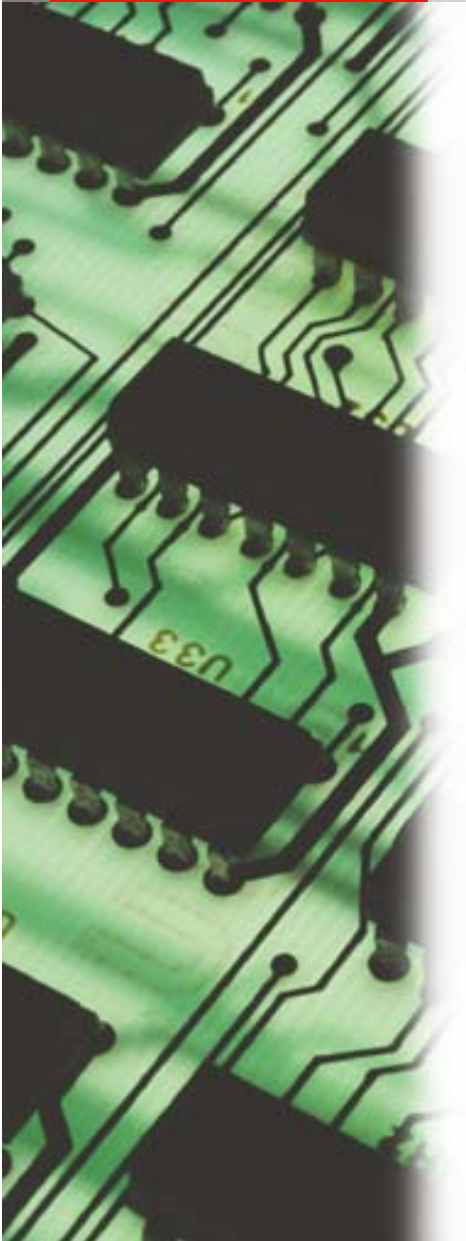
Normal Accident Theory (NAT)

- 
- NAT has grown out of work done by Charles Perrow—
begun in the aftermath of the Three Mile Island
nuclear accident
 - Fundamental premise:
 - “...organizations that aspire to failure-free performance are
inevitably doomed to fail because of inherent risks in the
technology that they operate.” [CAIB Report page 180]

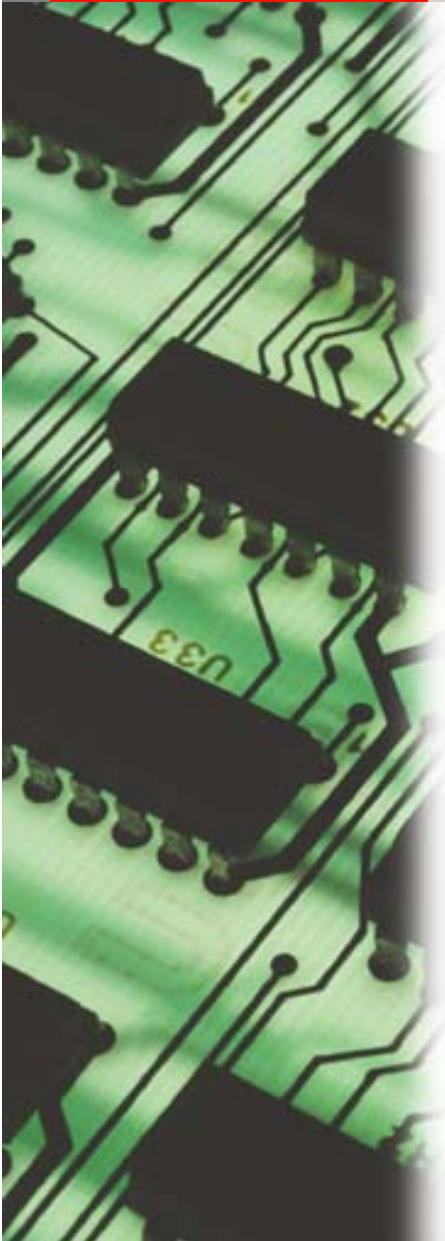
NAT (contd.)

- 
- If this were all that NAT said, it would be difficult to use in improving safety and project management—fortunately that is not the case
 - NAT provides important systems approaches and systems thinking that can inform safety and project management

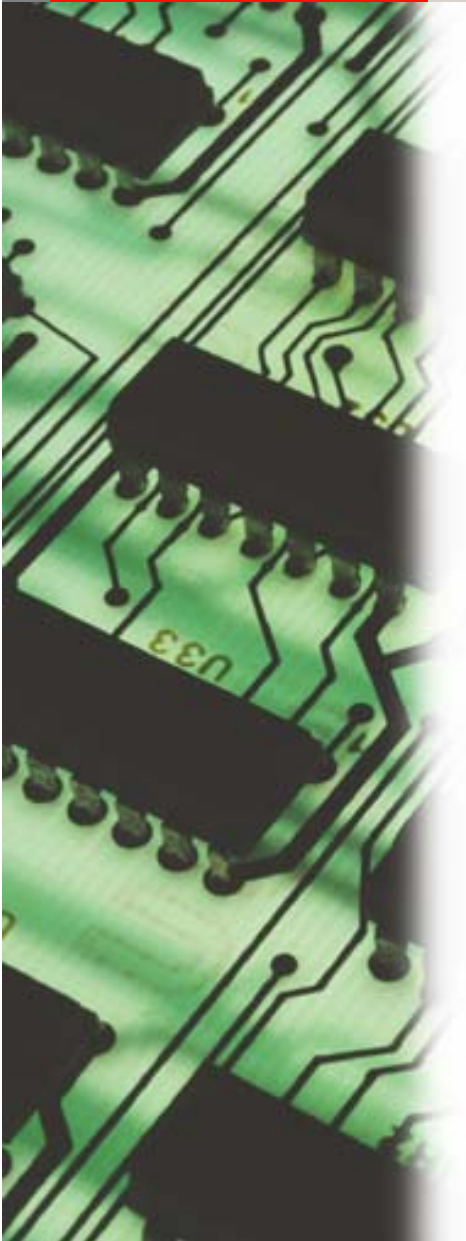
NAT—Systems Thinking

- 
- NAT introduced a six-element model of complex systems [Perrow 1999, page 8]:
 - Design of the system
 - The Equipment that makes up the system
 - Procedures used to operate the system
 - The Operators of the system
 - Supplies and materials that make up the equipment
 - The Environment in which the system operates
 - The model was, thus, designated DEPOSE

NAT—Systems Thinking (contd.)

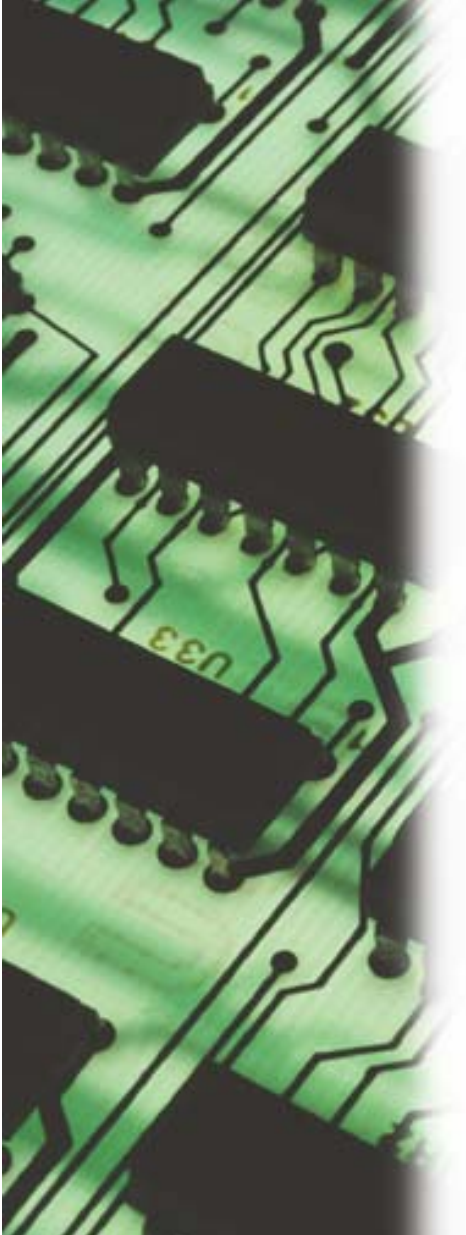
- 
- DEPOSE model provides a means to compare complex systems (e.g. emphasis placed on each of the six attributes)
 - Also can provide “bins” for evaluating causes of failures when they occur
 - “...perhaps the most original aspect of [NAT] is that it focuses on the properties of the systems...” [Perrow 1999, page 63]

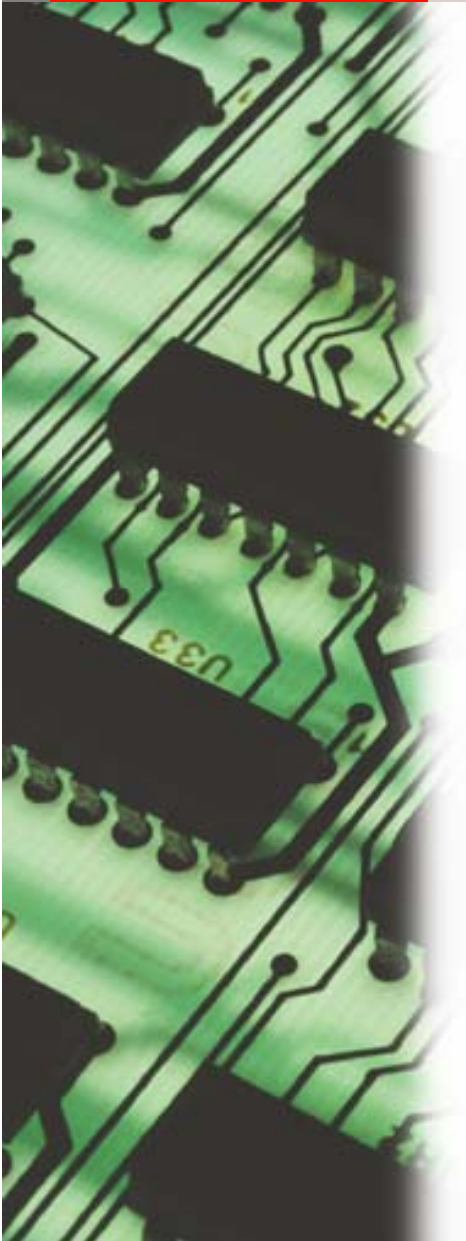
NAT—A systems approach

- 
- Definitions are fundamental to the NAT approach:
 - System
 - Incident
 - Accident
 - Component failure accident
 - System accident
 - Are all defined so as to produce an internally coherent framework
 - A hierarchy of “victims” is also introduced, “direct operators” through “progeny”

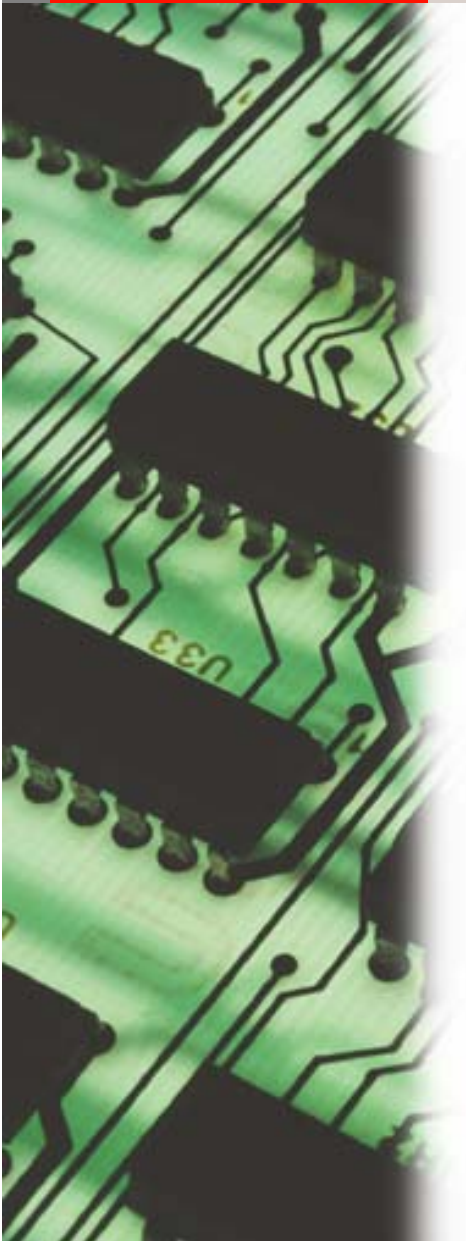
NAT—A systems approach (contd.)

- NAT defines two overarching dichotomies:
 - “Linear” versus “complex” systems
 - “Loose” versus “tight” coupling



- 
- DEPOSE can be used to inform system design and analysis, beginning early on in the project
 - Language of NAT can inform accident analysis
 - Systems engineering should favor:
 - Linear systems over complex
 - Loose coupling over tight coupling

NAT—A final word



“...sensible living with risky systems means keeping controversies alive, listening to the public, and recognizing the essentially political nature of risk assessment.”

(Perrow 1999, page 306)

High Reliability Organization (HRO)



- In contrast with NAT, HRO has as its basis:
 - “Organizations operating high-risk technologies, if properly designed and managed, can compensate for inevitable human shortcomings, and, therefore, avoid mistakes that under other circumstances would lead to catastrophic failures”
- Major work done by LaPorte and others

Institutional Constancy



- Describes the attributes of an organization that can effectively manage high-risk technologies over a long time period.
- Two major avenues by which organizations build institutional constancy:
 - Demonstrate that they are trustworthy
 - Show that they are capable of executing programs assigned to them



- How is trustworthiness to be demonstrated?
- Studies indicate four attributes of organizations that have successfully managed high-risk technologies, over the long term:
 - Formal, written goals with respect to their programmatic and safety performance
 - A consistent, strong articulation of their long-term vision
 - The development and fostering of strong institutional norms and processes
 - Systems of vigorous external enforcement or oversight

Capacity to Perform



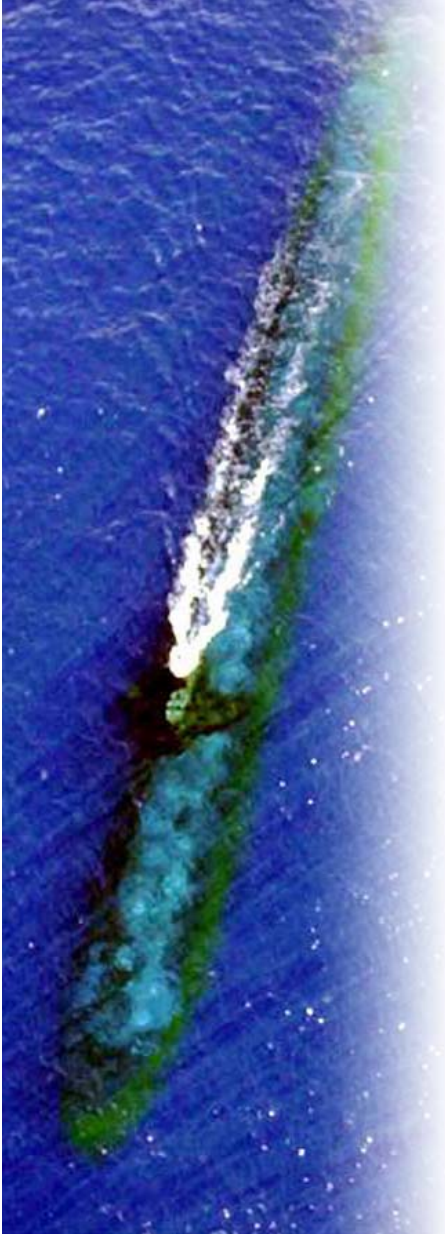
- Three major attributes are described as necessary for an organization to have the capacity to reliably enact programs
 - Adequate technical and administrative capability to assure performance
 - Analytical support structures that demonstrably incorporate the interests of the future
 - An effective capacity to detect and remedy failures—early in their development

HRO—So What?

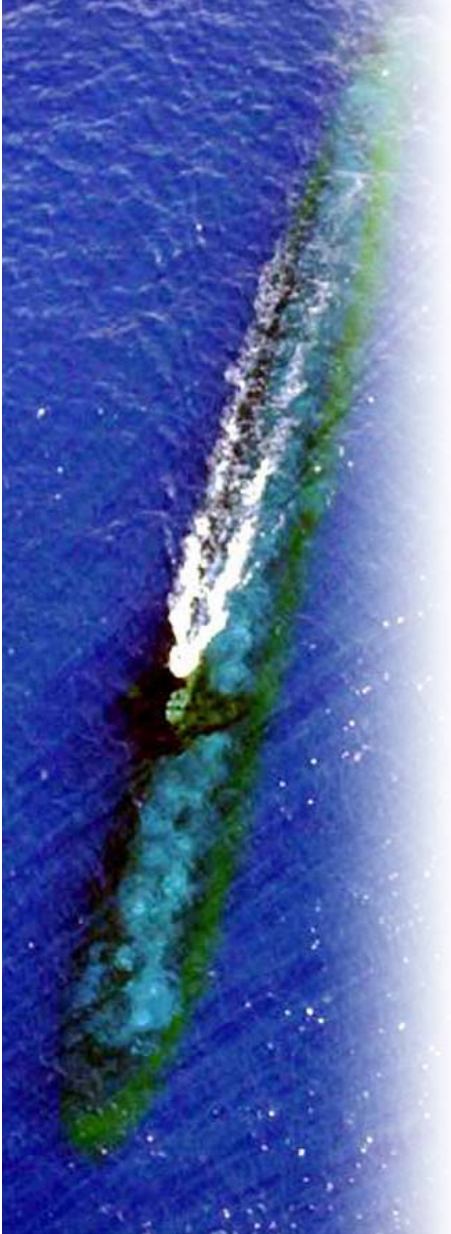


- General theoretical construct—could describe any successful organization.
- La Porte presented HRO as a tool to start discussion—not the “final answer.”
- He urged its use in case studies of highly reliable organizations to see if it “fit”
- Just such a case study was done of the Naval Reactors program (NR)

NR—High Reliability Organization?

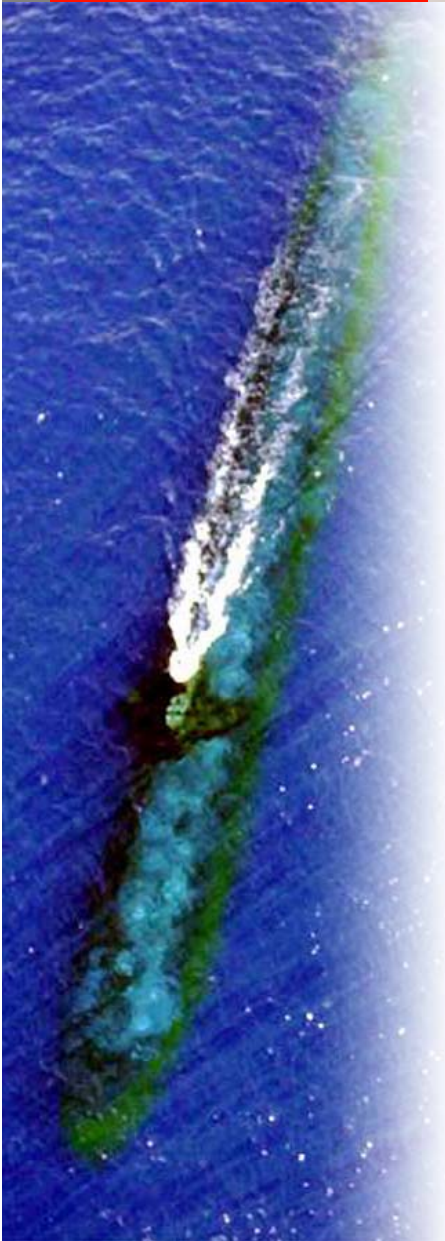


- NR was one of two government organizations that the CAIB described as exemplary
- Ships designed and built by the program have “more than 5,500 reactor years of experience without a reactor accident”
- Admiral Rickover described the program’s responsibilities for its reactors as “from the cradle to the grave”

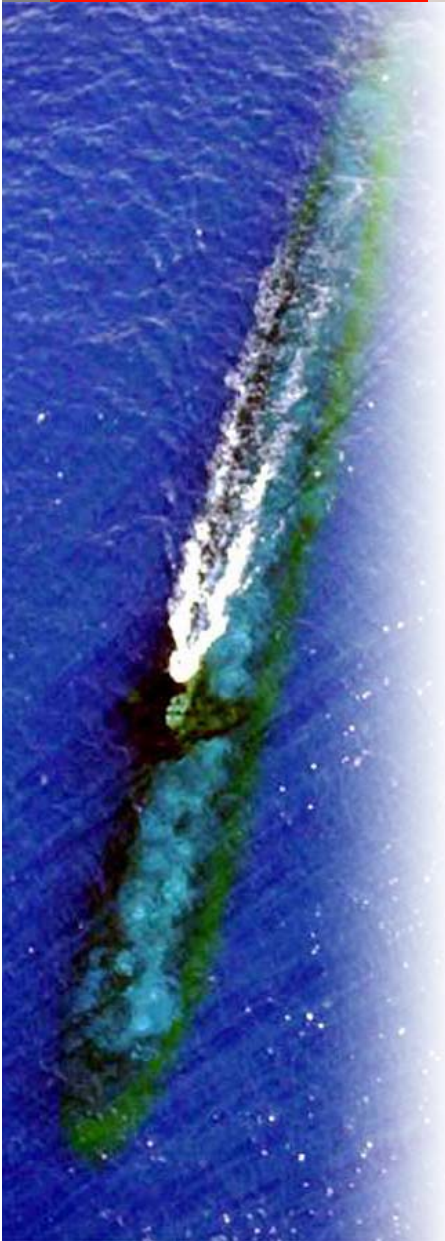


- Formal, written goals—have been a backbone of the program since inception:
 - A formal tasking from CNO launched the program
 - Standards and specifications for reactor plant development, manufacture and construction
 - Many have to do with health and safety (e.g. “no significant discharges of radioactivity to the environment”)
- “Cradle to grave” responsibility for the reactor plants illustrates the program’s commitment to constancy

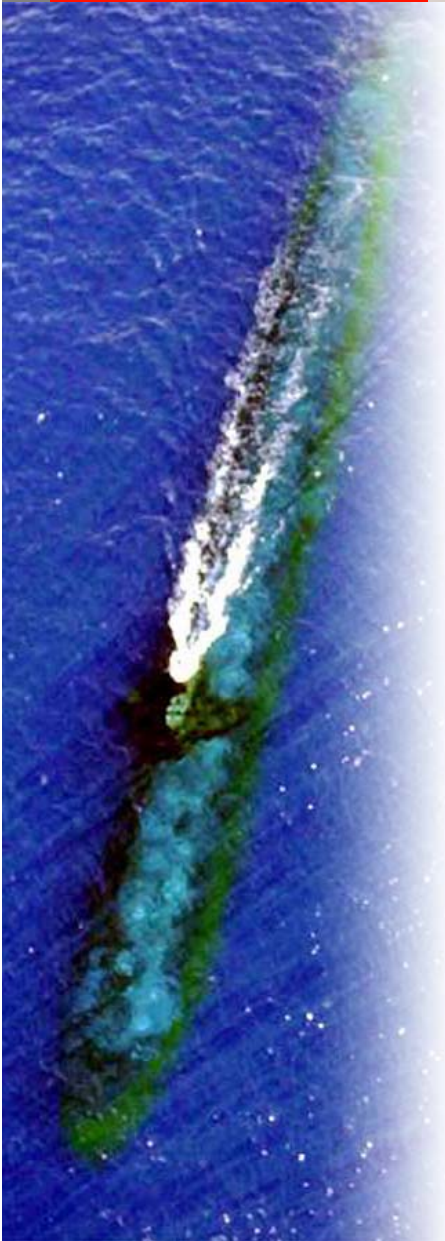
NR and Trustworthiness (contd.)

- 
- Strong institutional norms and processes
 - Personal responsibility
 - Field managers groomed in headquarters
 - Technical work ethic: attention to detail, adherence to consensus/program standards, technical inquisitiveness
 - Vigorous enforcement/oversight
 - NR (like NASA) born before today's regulatory structure
 - Self-regulating, but has used the NRC's Advisory Committee on Reactor Safeguards for design oversight
 - In 1980's opened the program to oversight from state and federal environmental agencies and has dedicated a group to ensure that these interfaces are satisfactory

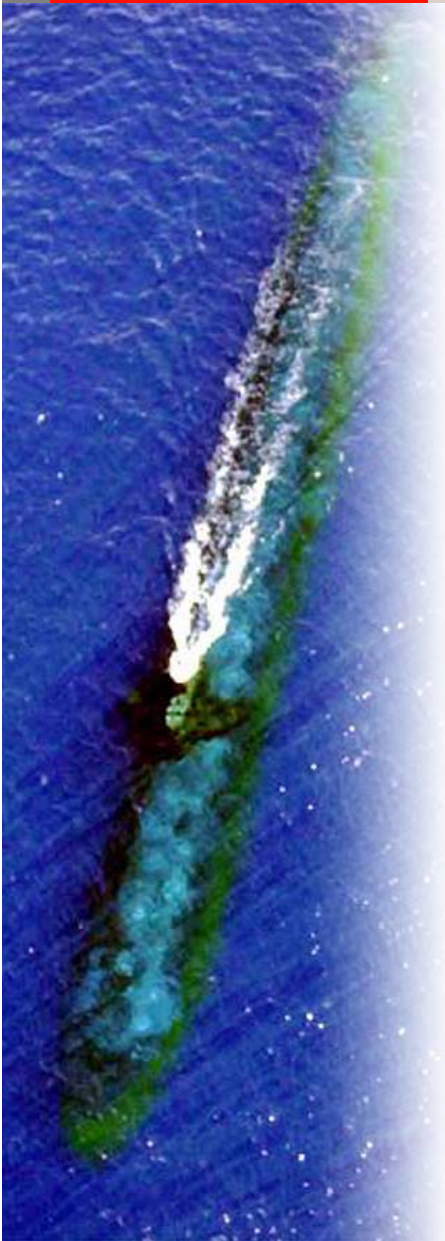
NR and Agency Capacity

- 
- A vertical, rectangular inset image on the left side of the slide. It shows an aerial view of a tropical island with a white sandy beach, green vegetation, and turquoise water. The image is oriented vertically, matching the text layout.
- Administrative and technical capability
 - Comprehensive administrative responsibility for the program (DOE and Navy)
 - Technical acumen in the government at least equal to that of its contractors
 - Control of personnel selection, training and qualification of personnel
 - Disciplined use of formal methods for decision making
 - Incorporating the interests of the future
 - Extensive attention paid to the selection of personnel and their career development
 - Life-cycle approach to systems design

NR and Agency Capacity (contd.)

- 
- Capacity to detect and remedy failures
 - Interlocking set of management reports
 - Special reporting systems to document operational and quality problems—all problems require formal, technical resolution with authoritative approval
 - Responses to system failures
 - Personnel issues
 - USS Thresher
 - “The Admiral” retires

NR “Lessons Learned”

- 
- Formality—the program’s emphasis on formal, written goals, standards and technical problem solving has been a hallmark.
 - Personnel—in developing and maintaining the capacity to execute its program, NR has understood that the major source of such capability is the men and women, both government and contractor, who are selected, trained and retained in the program. It is their acumen and commitment that makes error detection responsive and keeps the program focused on the future.

Overall NAT and HRO “Takeaways” for Project Management

- Failures will occur
 - NAT systems approach can help drive a philosophy that the goal of safety, reliability and maintainability analysis is to limit the impact of failures
 - NAT accident definitions assist in communicating risks
 - Feedback loops encouraged by HRO provide processes for limiting scope of failures



Overall NAT and HRO “Takeaways” for Project Management (contd.)



- Organizations managing high-risk technologies must develop and actively manage “trust”
 - If we understand “risk” why worry about “trust”
 - In government programs risk has an essential political element

Overall NAT and HRO “Takeaways” for Project Management (contd.)

- Strong technical competency is vital
 - Federal competence versus “contracting out”
 - Maintaining competence over the life cycle of a program



Additional Reading



- Bowman, F. (2003), "The Naval Nuclear Propulsion Program," statement before the House Science Committee (October 23, 2003)
- Columbia Accident Investigation Board (CAIB), *Report* (August 2003)
- Crawford, J. and Krahn, S. (1998a), "The Naval Nuclear Propulsion Program: A Brief Case Study in Institutional Constancy," *Public Administration Review*, Volume 58, pp 159-166
- Crawford, J. and Krahn, S. (1998b), "The Demanding Customer and the Hollow Organization: Meeting Today's Contract Management Challenge," *Public Productivity & Management Review*, Volume 22, pp 107-118
- LaPorte, T. and Consolini, P. (1991), "Working in Practice but Not in Theory: Theoretical Challenges of High Reliability Organizations," *Journal of Public Administration Theory and Practice*, Volume 1, pp. 19-47
- LaPorte, T. and Metlay, D. (1996), "Facing a Deficit of Trust: Hazards and Institutional Trustworthiness," *Public Administration Review*, Volume 56, pp 341-347
- LaPorte, T. and Keller, A. (1996), "Assuring Institutional Constancy: Requisite for Managing Long-Lived Hazards," *Public Administration Review*, Volume 56, pp 535-543
- Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies*, New York, Basic Books
- U. S. Congress (1965), "Loss of USS Thresher," hearings before the Joint Committee on Atomic Energy, Washington, DC, U. S. Government Printing Office